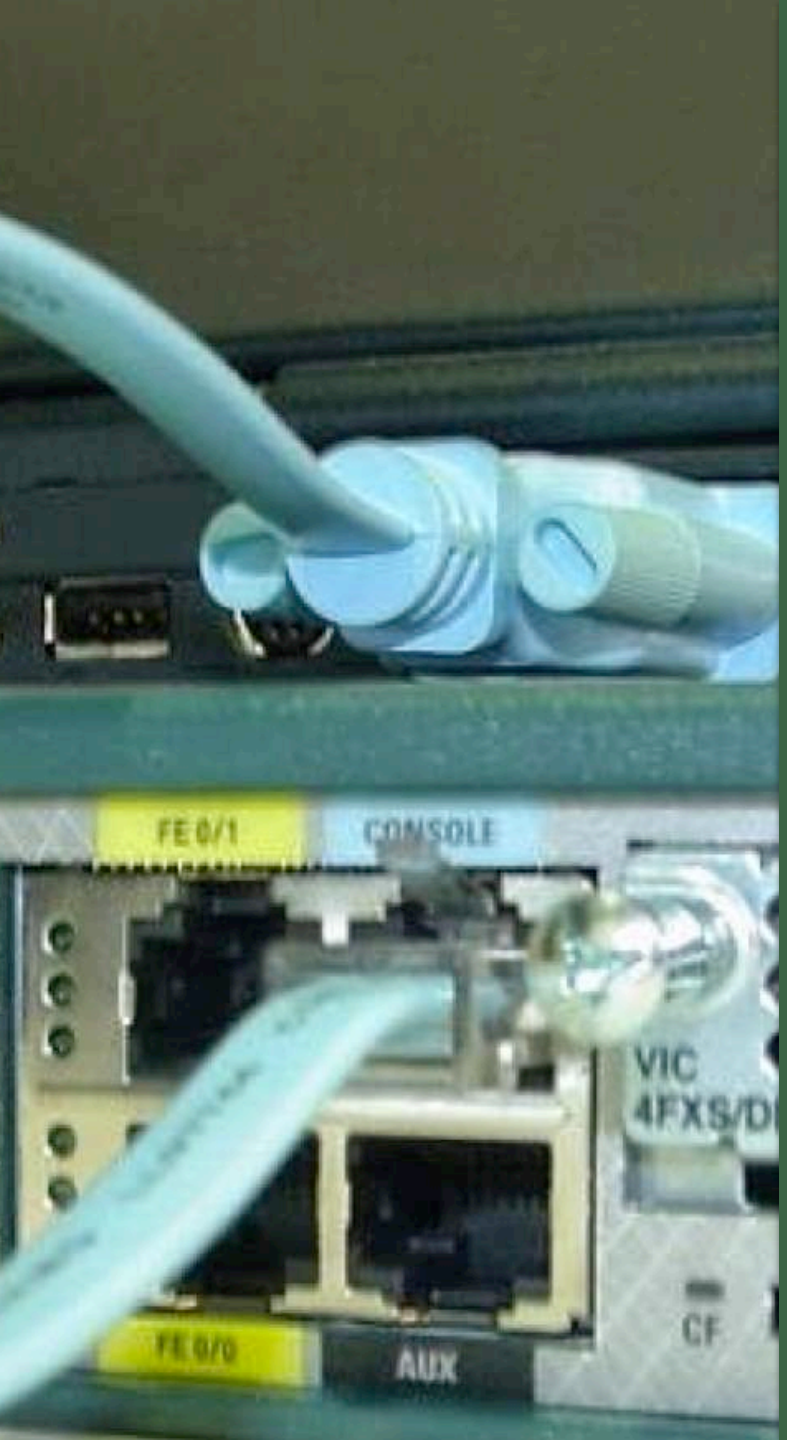


Universidad Autónoma del Estado de México
Centro Universitario UAEM Zumpango
Ingeniería en Computación

Instalaciones y equipos

M.T.I. Carlos Alberto Rojas Hernández

Agosto 2017

CENTRO UNIVERSITARIO UAEM ZUMPANGO

CENTRO UNIVERSITARIO UAEM ZUMPANGO
INGENIERÍA EN COMPUTACIÓN

Identificación de la Unidad de Aprendizaje (UA)

Nombre UA:

Instalaciones y equipos (L41078)

Total de horas a la semana: **3** Créditos: **5**

Carácter de la UA: **Optativa**

Modalidad: **Presencial**

UA Antecedente: **Ninguna**

UA Consecuente: **Ninguna**

M.T.I. Carlos Alberto Rojas Hernández

Presentación UA

Una de las principales actividades que tiene que desarrollar y enfrentar el ingeniero en computación, es el conocer a la perfección el elemento con el cual trabajará y desarrollará la mayoría de sus actividades, es por ello que requiere de conocimientos firmes para que pueda incursionar en ámbito en el cual debe dominar como es el de la conexión y equipo relacionado al área de redes.

Presentación UA

Dicha tecnología se encuentra tan cambiante en cuestiones de tiempo por lo tanto además de conocerlo tiene que actualizarse constantemente en su vida profesional.

Propósito UA

El alumno:

Aplicará el conocimiento adquirido en la teoría complementándolo con el del laboratorio, para poder configurar cualquier instalación de equipo de cómputo o bien de redes que se relacionen a sus actividades dentro y fuera del aula de clase.

Unidades de competencia

1. Conocer los diferentes componentes de un equipo de cómputo como son servidores, ruteadores, swiches, access points, pbx, acopladores de medios y todos los periféricos que integra una red.
2. Conocer e instalar los diagramas eléctricos, digitales, de cableado estructurado, basando en normas y estándares y realización de memorias técnicas con desarrollo de presupuestos para la realización de una red.
3. Conocer los sistemas que involucran un centro de cómputo y todo lo que pueda ser parte de dicho ambiente.
4. Conocer y establecer el concepto costo / beneficio en la instalación de una red LAN (sic) y equipo que la integra.

Unidades de competencia 1

Conocer los diferentes componentes de un equipo de cómputo como son servidores, ruteadores, swiches, access points, pbx, acopladores de medios y todos los periféricos que integra una red.

Unidad de competencia 1

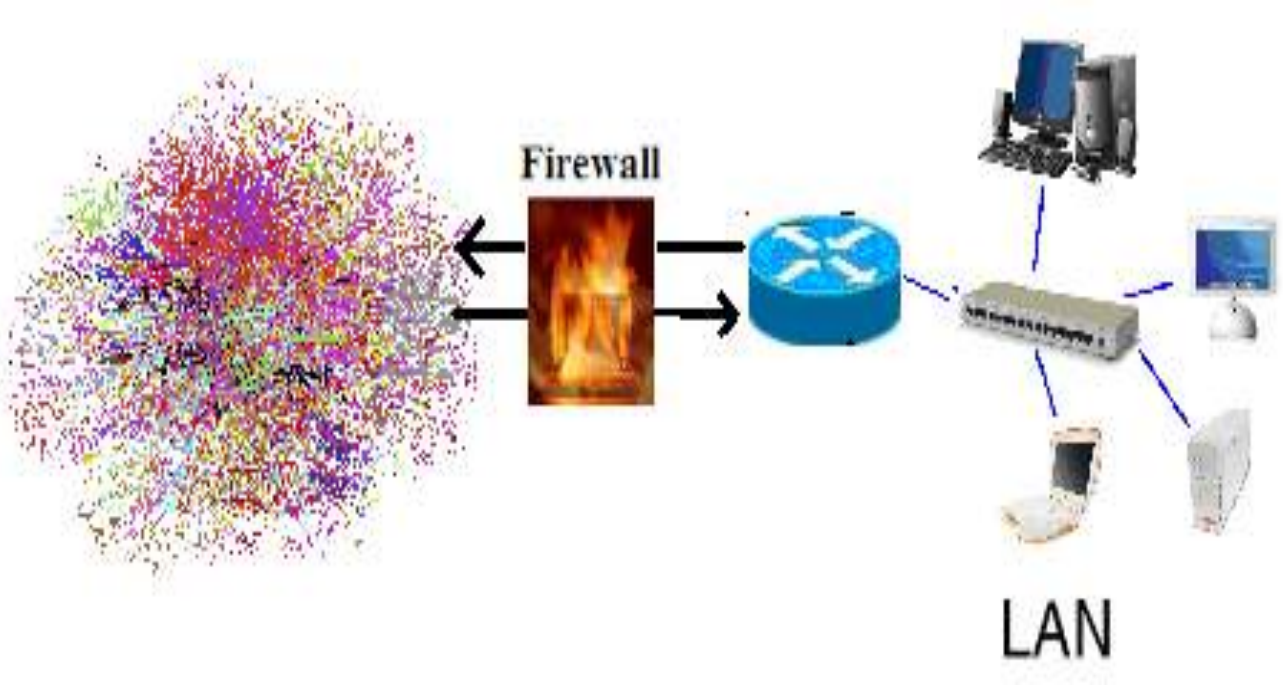
- Características de tipos de servidores, Lógicas, Físicas. .
- Características de de tipos de ruteadores.
- Características de de tipos de swiches.
- Características de Equipo detectores de intrusos.
- Características de Analizadores de contenido.
- Características de Firewall.
- Características de Acces Points.
- Características dde PBX / IP
- Características de Voz / IP.
- Características de Videoconferencia.
- Características de Acopladores de medios.

Características de Firewall

Existen elementos de hardware que son usados en las redes de datos para tratar de bloquear amenazas o ataques hacia nuestra red, actualmente entre los más utilizados se pueden mencionar los Firewall.

Características de Firewall

Separación lógica



Características de Firewall

¿ Qué es un Firewall?

Un Firewall , cortafuegos o muro de fuego es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre dos redes.

Características de Firewall

UAEM

¿ Qué es un Firewall?

De una forma más clara, podemos definir un cortafuegos como cualquier sistema (desde un simple router hasta varias redes en serie) utilizado para separar una máquina o subred del resto, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad.

Características de Firewall

UAEM

¿ Qué es un Firewall?

Los firewalls pueden ser implementados tanto en el hardware como en el software, o bien combinando los dos.

CENTRO UNIVERSITARIO UAEM ZUMPANGO

M.T.I. Carlos Alberto Rojas Hernández

CENTRO UNIVERSITARIO UAEM ZUMPANGO
INGENIERÍA EN COMPUTACIÓN

Características de Firewall

UAEM

¿ Qué es un Firewall?

Todos los mensajes que entran o salen de la intranet pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplen las políticas de seguridad especificados.

Características de Firewall

¿ Qué es un Firewall?

Las políticas de seguridad son el conjunto de reglas de seguridad, convenciones y procedimientos que gobiernan las comunicaciones dentro y fuera de una red.

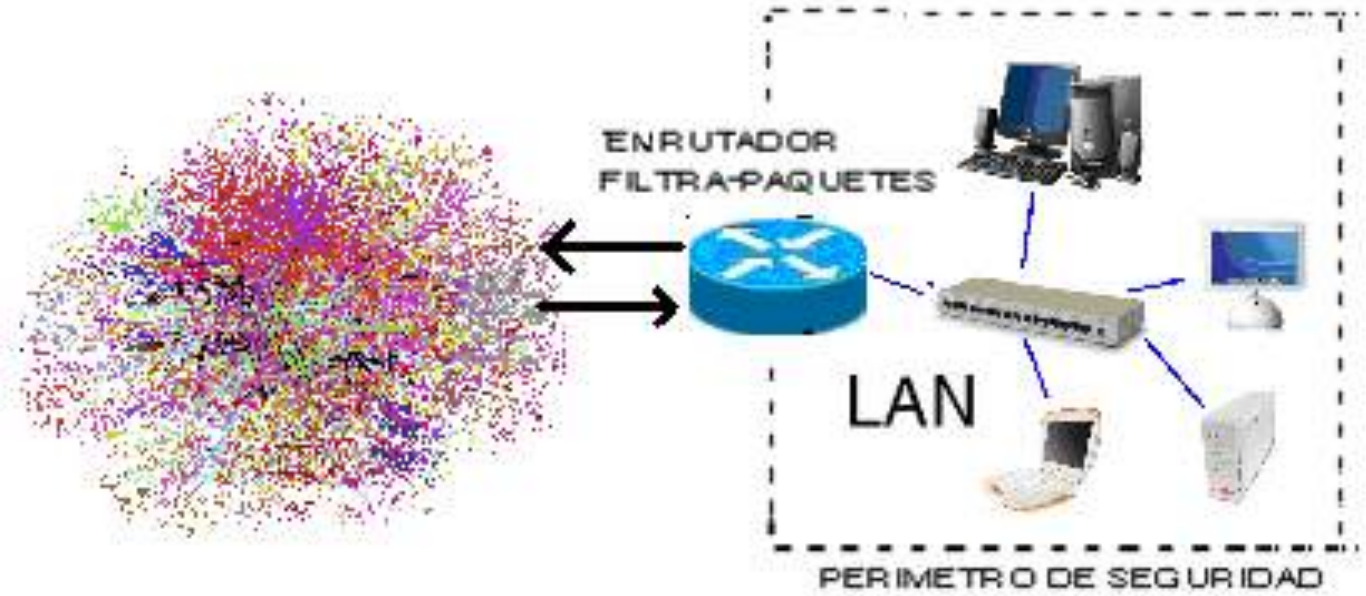
Características de Firewall

Existen cuatro técnicas para implementar un Firewall “físicamente”:

- Filtros a nivel paquete (Packet Filters)
- Firewall a nivel circuito (Circuit Level Firewalls)
- Firewall a nivel aplicación (Application Layer Firewalls)
- Filtros dinámicos a nivel paquete (Dynamic Packet Filters)

Características de Firewall

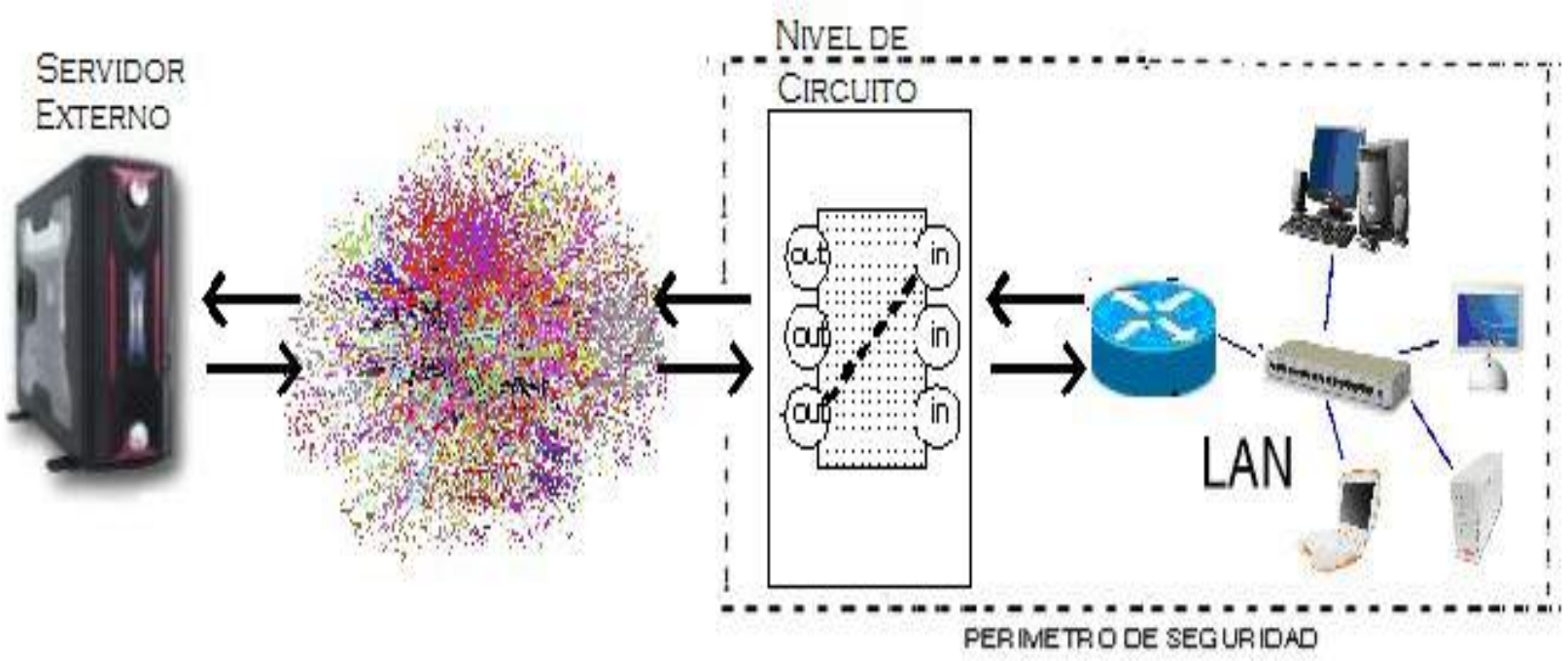
Filtros a nivel paquete (Packet Filters)



M.T.I. Carlos Alberto Rojas Hernández

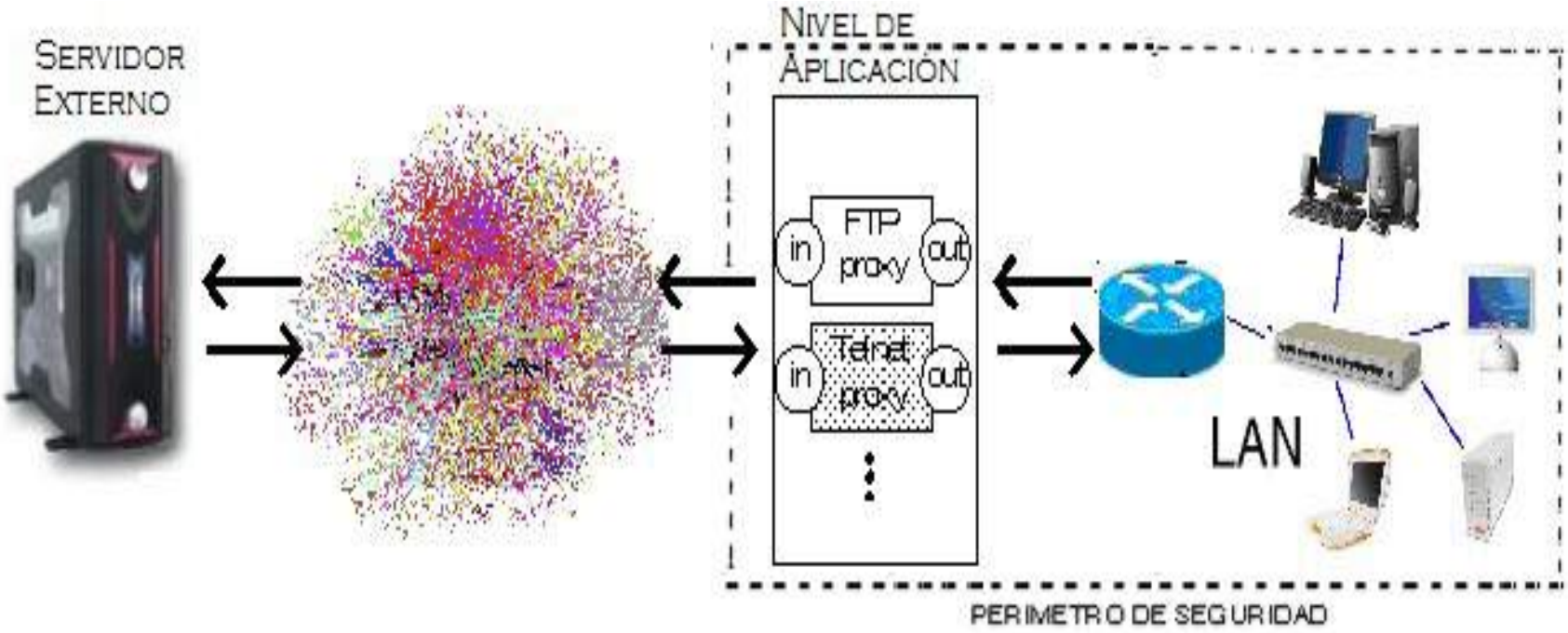
Características de Firewall

Firewall a nivel circuito (Circuit Level Firewalls)

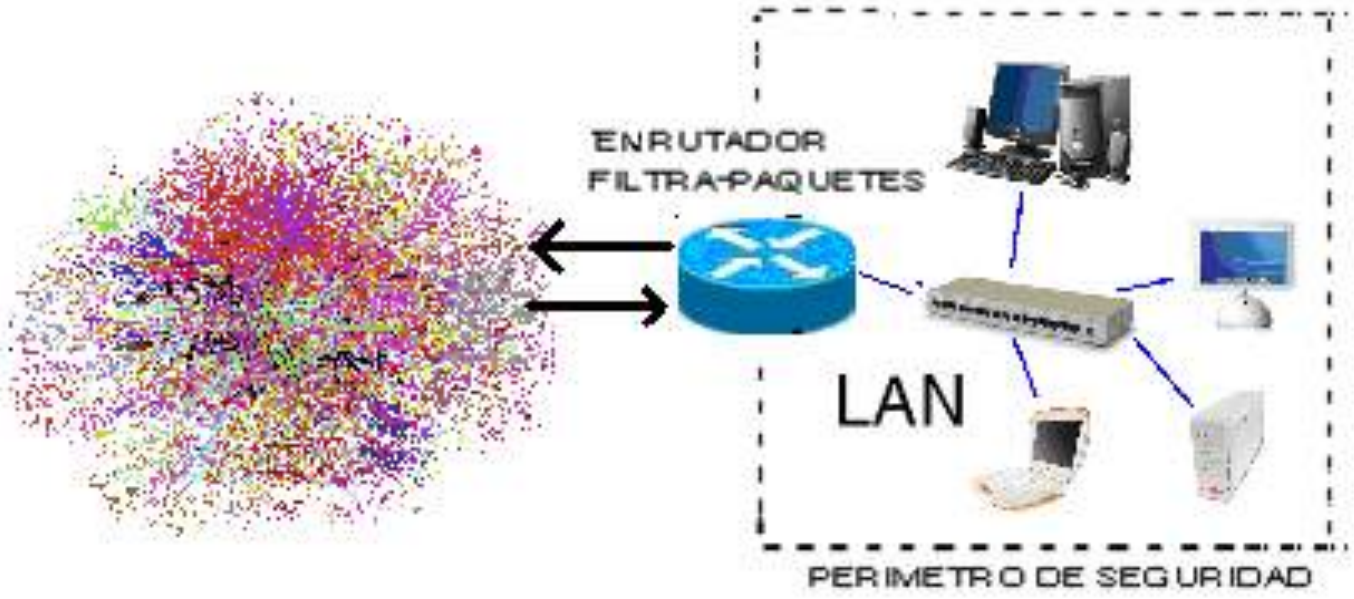


Características de Firewall

Firewall a nivel aplicación (Application Layer Firewalls)



Filtros dinámicos a nivel paquete (Dynamic Packet Filters)



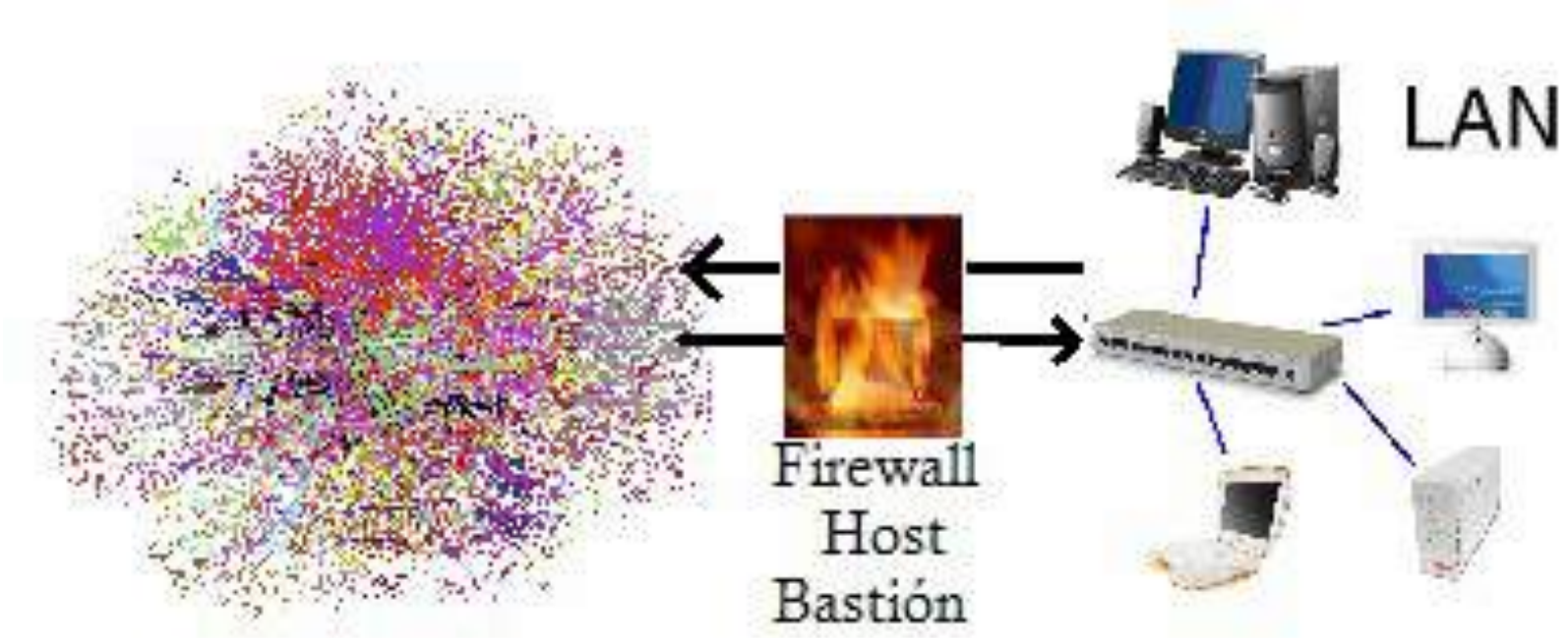
Características de Firewall

Además existen cuatro topologías de en donde se coloca el firewall

- Host bastión
- Router con filtrado (Screened Router)
- Firewall mediante filtrado de host (Screened Host)
- Firewall mediante filtrado de subred (Screened Subnet)

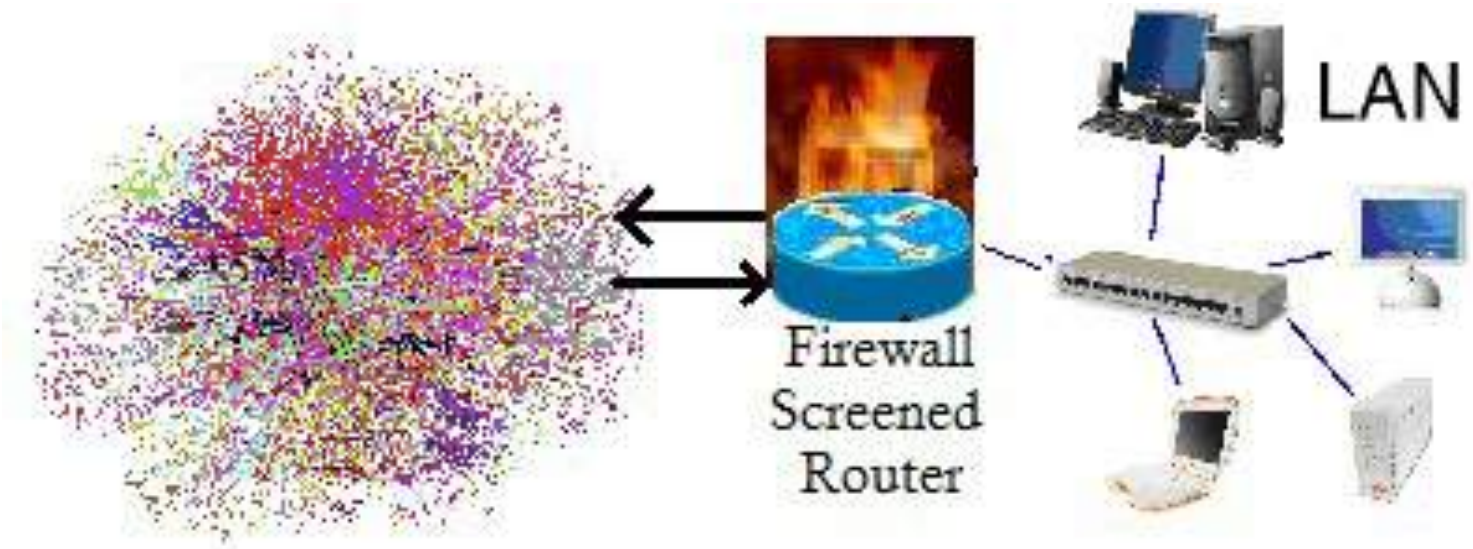
Características de Firewall

Host bastión



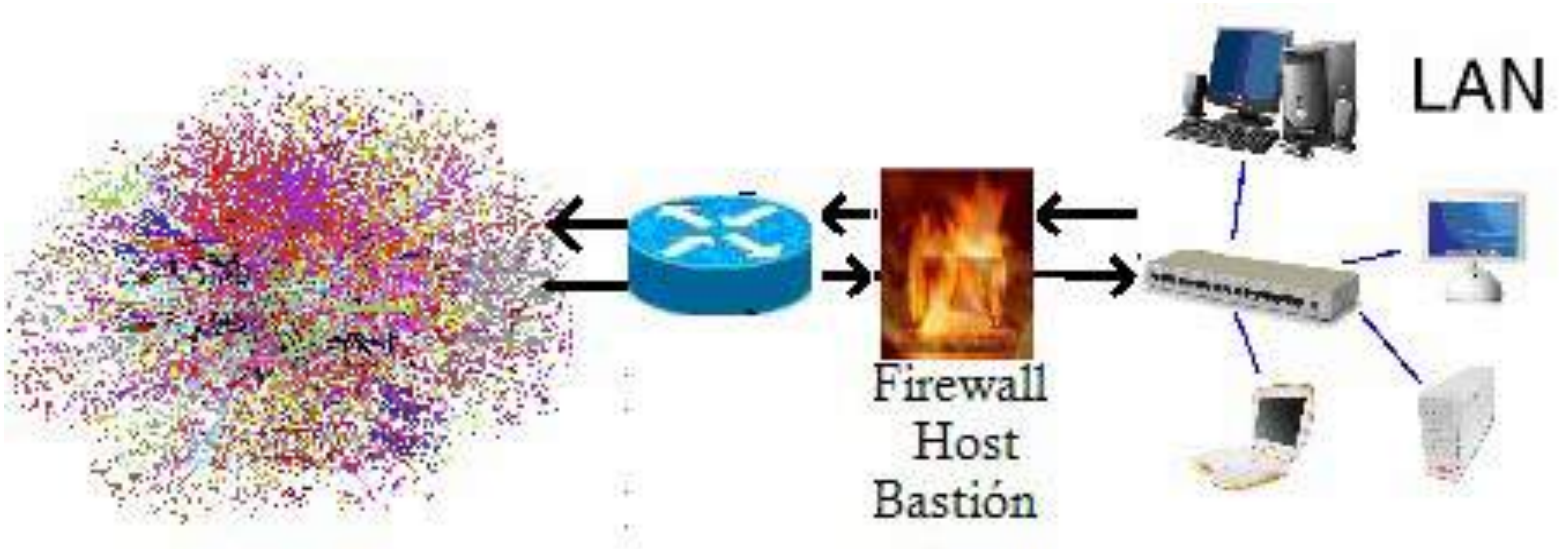
Características de Firewall

Router con filtrado (Screened Router)



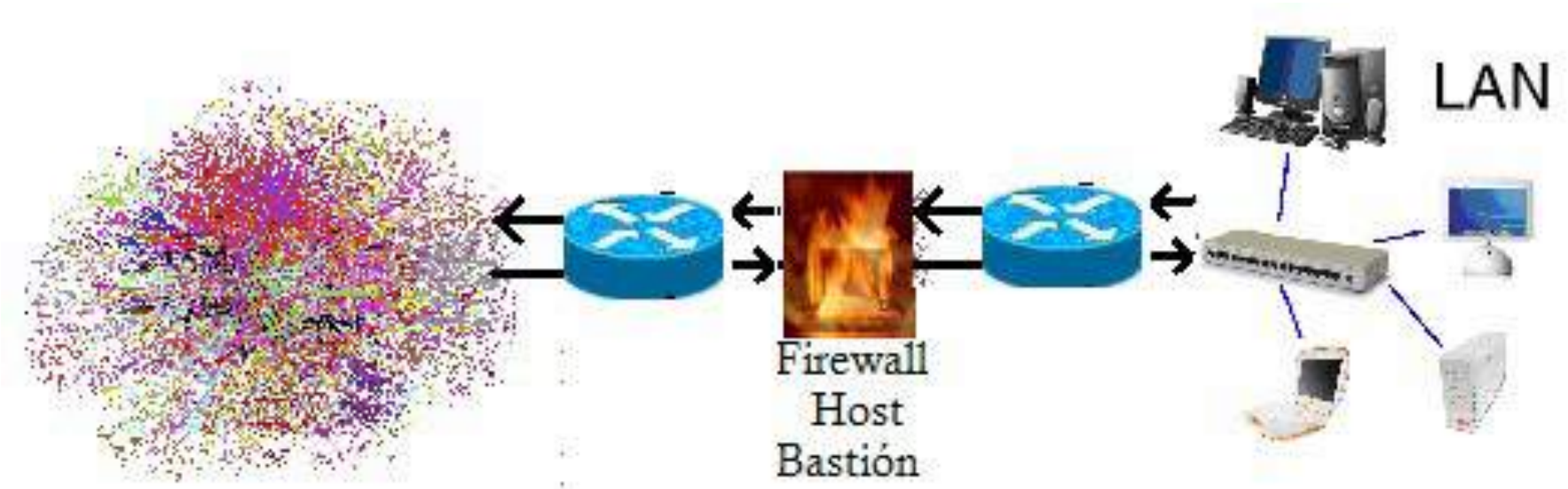
Características de Firewall

Firewall mediante filtrado de host (Screened Host)



UAEM

Firewall mediante filtrado de subred (Screened Subnet)



Características de Firewall

La topologías mencionadas anteriormente son útiles en cuanto a las redes de datos, sin embargo existen programas que solo se limitan a la protección de los equipos de manera individual, son productos relativamente nuevos, que por su facilidad de uso pueden instalados en computadoras personales por usuarios principiantes y expertos.

Firewalls personales

Principalmente son recomendados para gente que no apaga su computadora y se encuentra conectada horas o dias a Internet desde su casa, esto abre la posibilidad de que ”alguien” robe información o que use la computadora para atacar a otros.

Características de Firewall

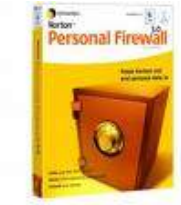
Podemos mencionar que las principal ventaja de los Firewall personales son:

Proteje el sistema operativo de ataques cuando se conecta a redes hostiles (Internet), si un virus del tipo backdoor se logro instalar se previene la conexión de este hacia el extrior e incluso cuando se utilizan nuevas aplicaciones se pueden ver las comunicaciones que se llevan a cabo.

Características de Firewall

Existen diferentes tipos y marcas de firewall personales, de hecho la mayoria de las “suites” de seguridad tiene como una aplicación estándar un antivirus y un firewall personal.

- McAfee Firewall
- ZoneAlarm
- Symantec Personal Firewall(Norton)
- Tiny Personal Firewall
- Panda Software
- Sygate



Características de Firewall

Cuando se toma la decisión de instalar un firewall se debe de tener muy en cuenta una serie de aspectos:

- Política de seguridad
- Determinar el nivel de vigilancia, redundancia y control.
- Financiamiento

Política de seguridad

"Todo lo que no es específicamente permitido está prohibido"

"Todo lo que no es específicamente prohibido está permitido"

Características de Firewall

UAEM

Política de seguridad

Para que nuestra política de seguridad sea la más adecuada de acuerdo a nuestras necesidades, debemos de tomar en cuenta que deben de tener ciertas características básicas.

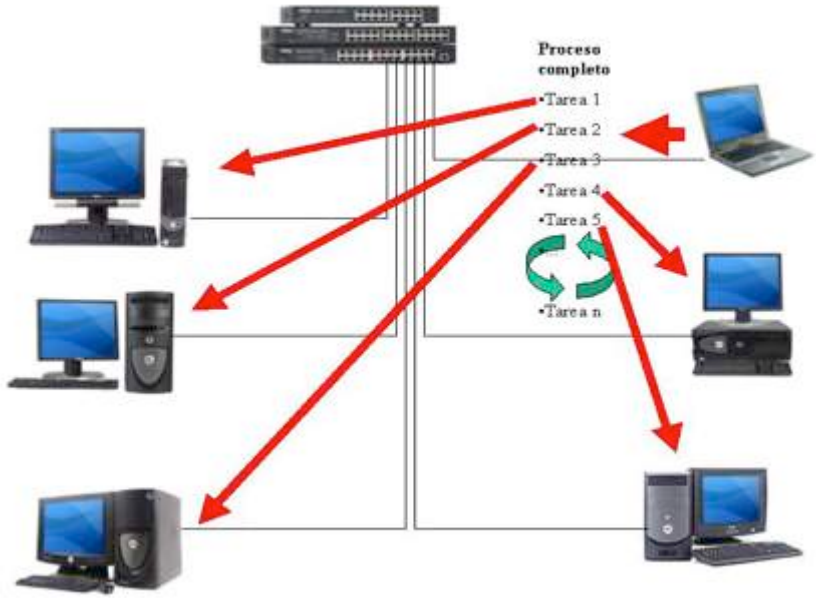
Podemos mencionar que tiene que seguir una serie de pasos bien definidos.

UAEM

Política de seguridad

Identificación

- Estudio del tráfico que circula por la red.
- Recolección de todos los servicios activos.



UAEM

Política de seguridad

Definición:

- Establecimiento de reglas generales
- Decisión de permitir o denegar el acceso

Política de seguridad

Implementación:

- Creación operativa de las reglas
- Aplicación al cortafuegos de las reglas

Política de seguridad

Verificación:

- Comprobación del buen funcionamiento de las reglas
- ! No denegar nada importante !

Política de seguridad

Documentación:

- Información de las reglas establecidas
- Aspecto a cumplir de forma estricta

UAEM

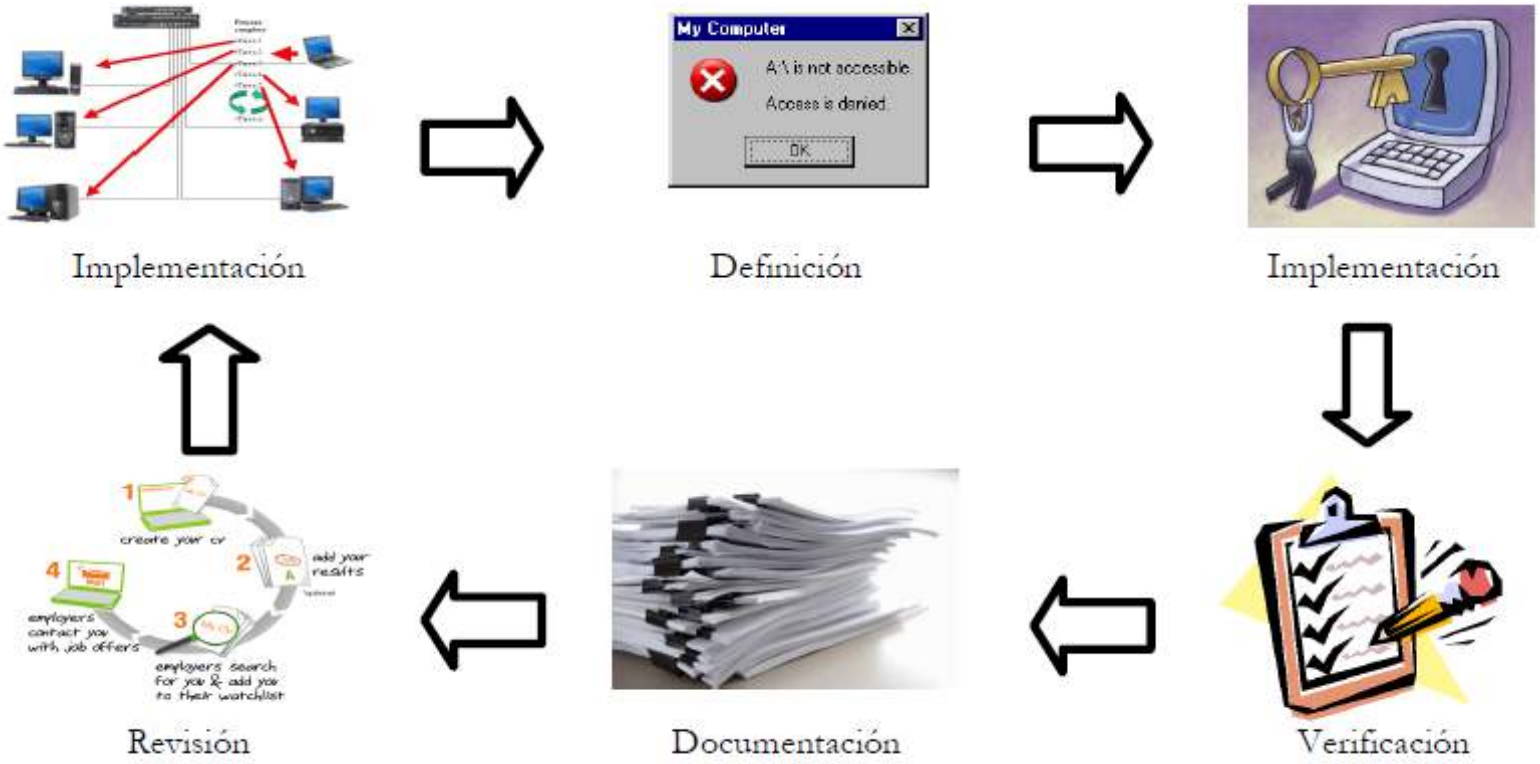
Política de seguridad

Revisión:

- Comprobar que las reglas funcionan correctamente
- Actualizar las reglas existentes

Características de Firewall

Política de seguridad



Características de Firewall

Cuando se toma la decisión de instalar un firewall se debe de tener muy en cuenta una serie de aspectos:

Política de seguridad
Determinar el nivel de vigilancia, redundancia y control.
Financiamiento

Características de Firewall

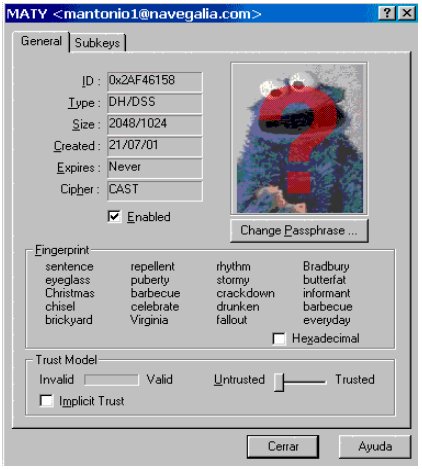
Determinar el nivel de vigilancia, redundancia y control.

Restricciones de dia y hora.

Características de Firewall

Determinar el nivel de vigilancia, redundancia y control.

Autentificación de usuarios

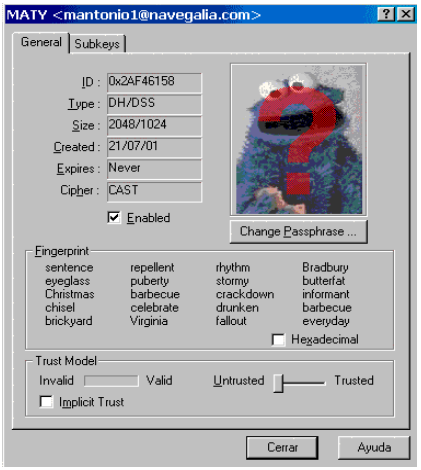


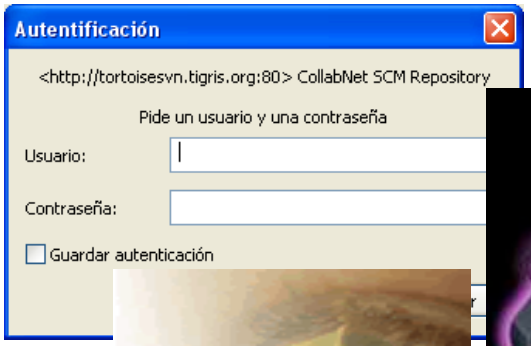
- Contraseñas
- Tarjetas inteligentes
- Perfiles biométricos

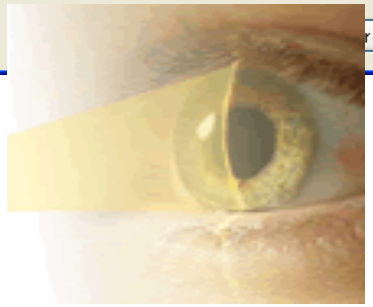
Características de Firewall

Determinar el nivel de vigilancia, redundancia y control.

Autentificación de usuarios

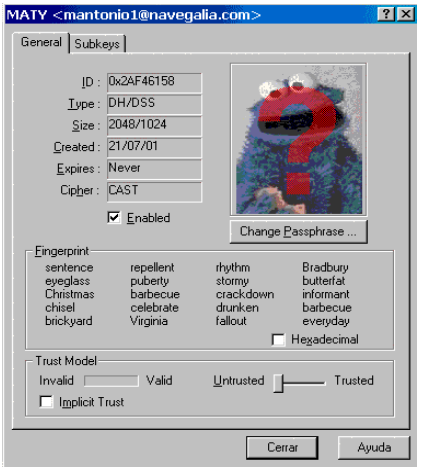






Características de Firewall

Determinar el nivel de vigilancia, redundancia y control.



Autentificación de usuarios

Características de Firewall

Determinar el nivel de vigilancia, redundancia y control.

Registro de operaciones

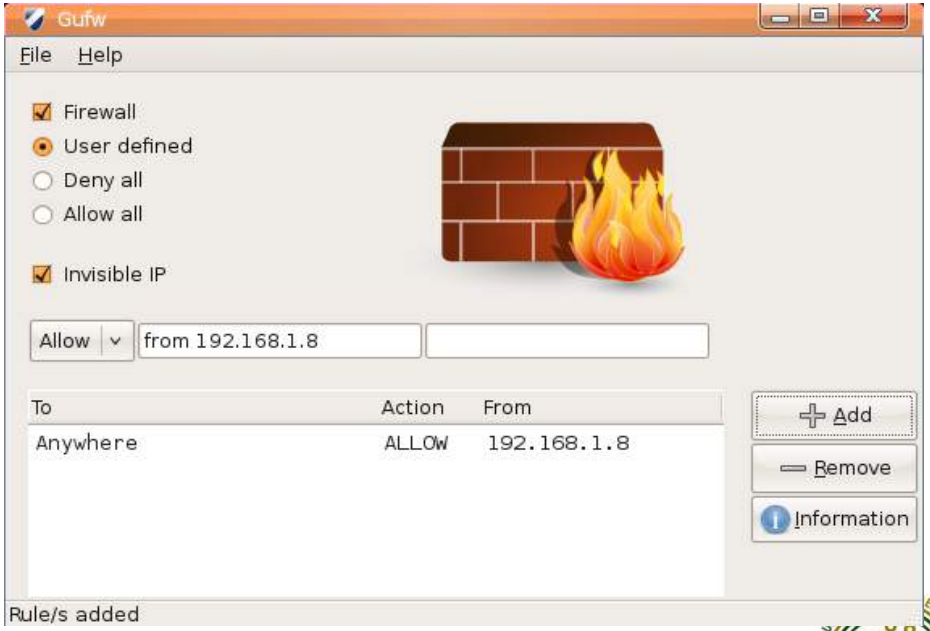
Información de filtrado, Direcciones IP destino y fuente, información de los paquetes, fecha y hora, puertos, acceso de intrusos...

Características de Firewall

Determinar el nivel de vigilancia, redundancia y control.

Interfaces de administración

- Interface basada en archivos de texto
- Interface basada en menús de
- GUI

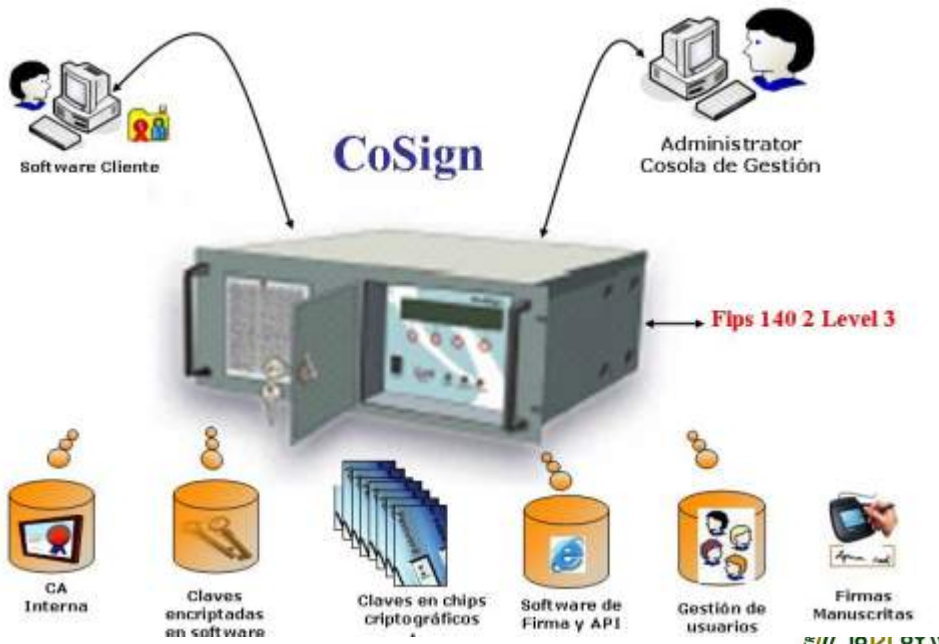


Características de Firewall

Determinar el nivel de vigilancia, redundancia y control.

Control de carga

Limitar la cantidad de conexiones simultaneas que una red o dispositivo pueden tener activas
(NO es control de ancho de banda)



Características de Firewall

Cuando se toma la decisión de instalar un firewall se debe de tener muy en cuenta una serie de aspectos:

Política de seguridad
Determinar el nivel de vigilancia, redundancia y control.
Financiamiento

Características de Firewall

UAEM

SONICWALL TZ 170 - Firewall

€ 155.16

Protocolo de conmutación	Ethernet
Red / Protocolo de transporte	TCP/IP, PPTP, UDP/IP, L2TP, ICMP/IP, IPSec, PPPoE
Protocolo de gestión remota	SNMP, HTTP, HTTPS
Rendimiento	Capacidad de pleno estado : 90 Mbps ¦ Capacidad de antivirus de pasarela : 8 Mbps ¦ Capacidad de prevención contra intrusiones : 8 Mbps ¦ Rendimiento 3DES y AES : 30+ Mbps
Capacidad	Nodos : 10 ¦ Túneles VPN (de sitio a sitio) : 2 ¦ Conexiones concurrentes : 6000 ¦ Políticas de seguridad : 100
Indicadores de estado	Actividad de enlace, alimentación, modo de prueba, dispositivo conectado a 100M
Características	Protección firewall, conmutación, soporte de DHCP, soporte de NAT, cifrado del hardware, asistencia técnica VPN, señal ascendente automática (MDI/MDI-X automático), prevención contra ataque de DoS (denegación de servicio), inspección profunda, soporte de gatekeeper VoIP, gestión de ancho de banda de salida VoIP
Algoritmo de cifrado	DES, Triple DES, AES, IKE
Método de autentificación	RADIUS, certificados X.509, base de datos de usuarios internos

Telefonía IP

Protocolos VoIP	H.323, SIP
Funciones de telefonía IP	Soporte de gatekeeper VoIP, gestión de ancho de banda de salida VoIP, seguimiento y monitorización de llamadas VoIP, gestión de ancho de banda entrante VoIP

Expansión / Conectividad

Interfaces	5 x nodo de red - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 1 x gestión - consola - RJ-45 ¦ 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN)

Características de Firewall

Fortinet 50B

$ 495 USD

Technical Specifications

HARDWARE SPECIFICATIONS	FortiGate-50B	FortiWiFi-50B
LAN Switching Interfaces	3	3
WAN Interfaces	2	2
DMZ Interfaces		
Analog Modem		
Wireless LAN		
802.11a/b/g		802.11 b/g
USB Ports	2	2
Power Over Ethernet (PoE)		Yes
PC Card Slot*		
Supported VDOMs	10	10

* PC card is sold separately

SYSTEM PERFORMANCE *		
Firewall Throughput	50 Mbps	50 Mbps
VPN IPSec Throughput	48 Mbps	48 Mbps
Antivirus Throughput	19 Mbps	19 Mbps
IPS Throughput	30 Mbps	30 Mbps
Dedicated IPSec VPN Tunnels	20	20
Unlimited User Licenses	Yes	Yes
Concurrent sessions	25,000	25,000
New Sessions/Second	2,000	2,000
Policies	2,000	2,000

Características de Firewall

UAEM

Cisco ASA 5505 Firewall Edition Bundle

$5,571.55

Procesador / Memoria / Almacenamiento	
RAM instalada (máx.)	256 MB
Memoria flash instalada (máx.)	64 MB Flash
Conexión de redes	
Factor de forma	Externo
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	IPSec
Rendimiento	Capacidad del cortafuegos : 150 Mbps ¦ Capacidad de la VPN : 100 Mbps
Capacidad	Peers VPN IPSec : 10 ¦ Peers VPN SSL : 2 ¦ Sesiones concurrentes : 10000
Características	Protección firewall, puerto DMZ, asistencia técnica VPN, soporte VLAN, montable en pared
Algoritmo de cifrado	Triple DES, AES, SSL
Expansión / Conectividad	
Total ranuras de expansión (libres)	1 (1) x Ranura de expansión
Interfaces	6 x red - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 2 x red / energía - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 3 x Hi-Speed USB - 4 PIN USB tipo A ¦ 1 x gestión - consola - RJ-45

CENTRO UNIVERSITARIO UAEM ZUMPANGO

INGENIERÍA EN COMPUTACIÓN

Características de Firewall

UAEM

Nortel Switched Firewall System 6616

Networking	
Form Factor	External
Ports Qty	12
Connectivity Technology	Wired
Data Link Protocol	Ethernet, Fast Ethernet, Gigabit Ethernet
Network / Transport Protocol	ICMP/IP
Routing Protocol	OSPF, RIP-1, RIP-2, IGMP, DVMRP, VRRP
Remote Management Protocol	Telnet, SNMP 3, SNMP 2c
Performance	Firewall throughput : 7 Gbps VPN throughput (3DES IPSec) : 88 Mbps
Capacity	Concurrent sessions : 2000000 Concurrent VPN tunnels : 25000
Features	Flow control, layer 3 switching, layer 2 switching, DHCP support, BOOTP support, ARP support, trunking, load balancing, VLAN support
Encryption Algorithm	SSL, TLS
Authentication Method	Secure Shell (SSH), Secure Shell v.2 (SSH2)
Compliant Standards	IEEE 802.2, IEEE 802.3z, IEEE 802.1Q, IEEE 802.3x
Expansion / Connectivity	
Expansion Slots Total (Free)	8 (8) x GBIC
Interfaces	8 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x management - RS-232C - 9 pin D-Sub (DB-9) 1 x management - RJ-45

$39,462.99 USD

CENTRO UNIVERSITARIO UAEM ZUMPANGO

INGENIERÍA EN COMPUTACIÓN

Características de Firewall

FortiGate-3810A-E4-Premium Complete Content Protection Bundle

$72,495 USD

Networking	
Form Factor	External
Connectivity Technology	Wired
Data Link Protocol	Ethernet, Fast Ethernet, Gigabit Ethernet
Network / Transport Protocol	PPTP, L2TP, IPSec, PPPoE, DHCP
Routing Protocol	OSPF, RIP-1, RIP-2, BGP
Remote Management Protocol	SNMP, Telnet, HTTP, HTTPS
Performance	Firewall throughput : 7 Gbps 3DES throughput : 1 Gbps Gateway anti-virus throughput : 500 Mbps
Capacity	Simultaneous users : unlimited Concurrent sessions : 2000000 Security policies : 100000 VPN tunnels : 10000
Status Indicators	Power
Features	Routing, DHCP support, NAT support, PAT support, VLAN support, Syslog support, traffic shaping, DoS attack prevention, Intrusion Detection System (IDS), E-mail alert, VPN passthrough, antivirus analysis, High Availability, Intrusion Prevention System (IPS), URL filtering, IP address filtering, Stateful Failover, Transparency, anti-spam protection, Dead Peer Detection (DPD), IPSec NAT-Traversal (NAT-T)
Encryption Algorithm	DES, Triple DES, MD5, AES, IKE, SSL, SHA-1
Authentication Method	SecurID, Secure Shell (SSH), RADIUS, LDAP, internal user database, Active Directory
Compliant Standards	IEEE 802.1Q
IP Telephony	

CENTRO UNIVERSITARIO UAEM ZUMPANGO

INGENIERÍA EN COMPUTACIÓN

Factores de riegos

- Mala configuración del Firewall

- Falsa sensasión de seguridad

- Centrar las medidas de protección en un solo sistema

- Elección erronea de las políticas de seguridad

Limitaciones

NO puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquettes o memorias flash y las substraigan del sistema o instalaciones.

Limitaciones

NO puede proteger contra los ataques de la "Ingeniería Social"

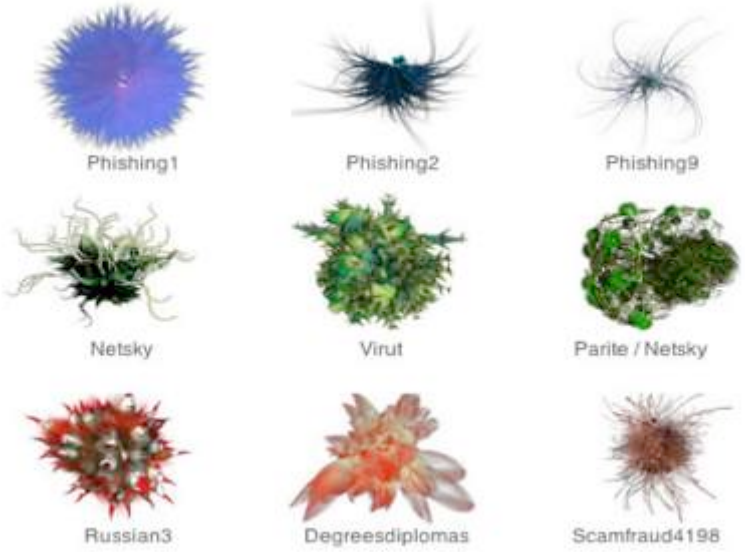
Ejemplo: Un hacker que pretende ser un supervisor y convence a un empleado nuevo de darle su contraseña.

Limitaciones

NO puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno. (Caballos de troya)

Limitaciones

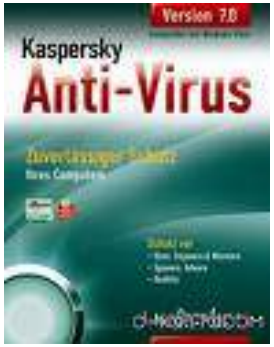
NO puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software.

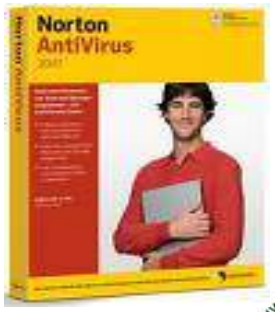


UAEM

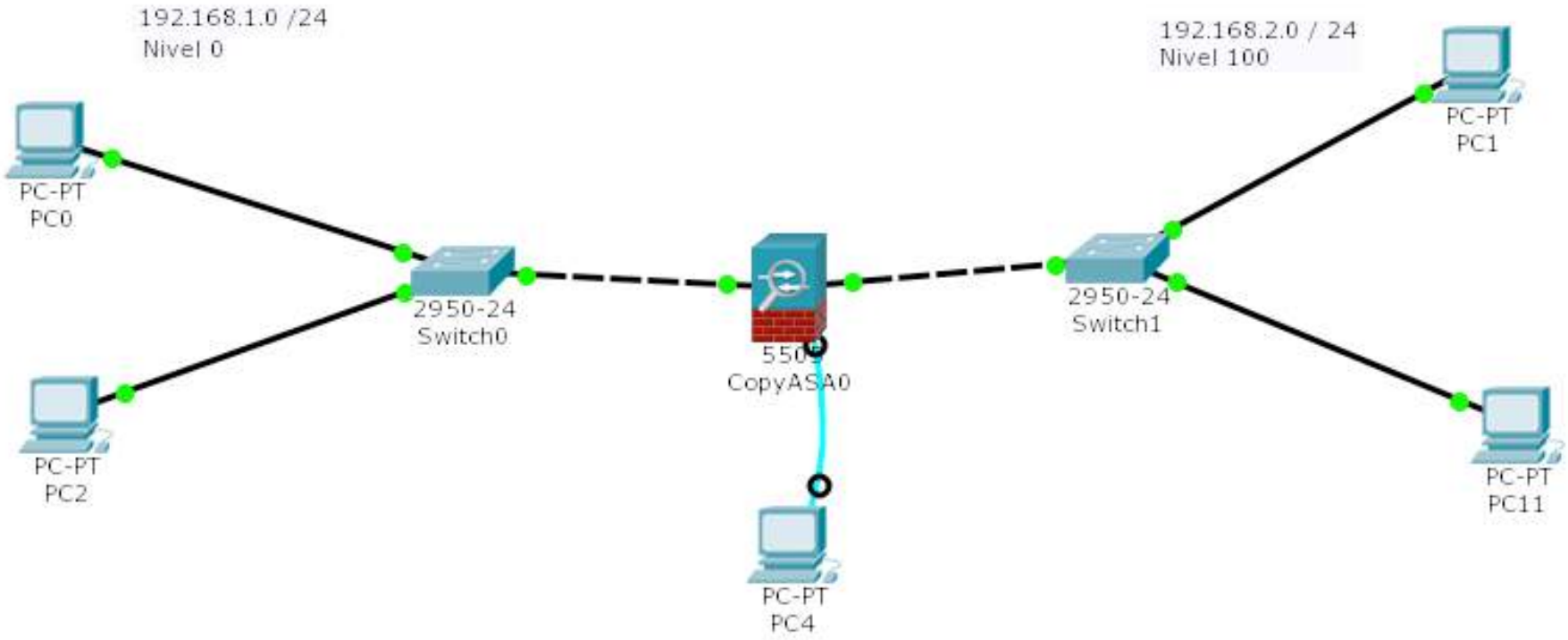
Limitaciones

“NO es un antivirus”





Configuración del Firewall



UAEM

Configuración del Firewall

Creación de VLAN

```
firewall# configure terminal
firewall(config)# interface vlan 1
firewall(config-if)# ip address 192.168.1.1
255.255.255.0
firewall(config-if)# exit
```

Los mismos comandos para vlan 2

UAEM

Configuración del Firewall

Asignación de puertos a la VLAN

```
firewall(config)# interface ethernet 0/1
firewall(config-if)# switchport access vlan 1
firewall(config-if)# no shutdown
firewall(config-if)# exit
```

Los mismos comandos para ethernet 0/2

UAEM

Configuración del Firewall

Asignación de políticas de seguridad

```
(config)# class-map inspection_default
(config-cmap)#match default-inspection-traffic
(config-cmap)#exit

(config)# policy-map global_policy
(config-pmap)class inspection_default
(config-pmap-c)inspect icmp
(config-pmap-c)exit

(config)# service-policy global_policy global
```

Referencias bibliográficas

[1] Andrew S. Tanenbaum, David J. Wetherall, “Redes de computadoras”, 5a edición, Pearson Educación, 2012, ISBN: 6073208170

[2] William Stallings, “Network security essentials : applications and standards”, 4th Edition, Prentice Hall, 2011, ISBN: 9780136108054

[3] Matias Katz, “Redes y seguridad”, Alfaomega, 2013, ISBN 9789871609284

Referencias bibliográficas

[4] Academia de Networking de Cisco Systems ,“Fundamentos de seguridad de redes especialista en Firewall Cisco”, 5a edición, Pearson Educación, 2005, ISBN: 9788420545400

[5] Greg Bastien, “CCSP Cisco secure PIX Firewall advanced exam certification guide”, 2da. Edición, Cisco, 2005, ISBN 1587201232

UAEM